UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/748,441	12/27/2000	Wolfgang Daum	9D-HR-19614-Daum et al	4179

7590 08/24/2005

John S. Beulick
Armstrong Teasdale LLP
ONE METROPOLITAN SQUARE
SUITE 2600
ST. LOUIS, MO 63102

EXAMINER	
DINH, MINH	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 08/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/748,441	DAUM ET AL.	
	Examiner	Art Unit	
	Minh Dinh	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 May 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *16-22,24,25 and 27-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *16-20,24,25 and 27-31* is/are rejected.

7)☒ Claim(s) *21 and 22* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 July 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed 05/18/2005. Claims 16-18, 20, 24-25 and 27-31 have been amended; claims 1-15, 23 and 26 have been cancelled.

Response to Arguments

2. Applicant's arguments filed 05/18/2005 with respect to claims 16, 25, 28 and 30 have been considered but are not persuasive. Applicant's amendments have necessitated a new search and new grounds of rejection.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 25, 27 and 30-31 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. Claim 25 is directed to a system in which communication between an appliance communication center and different appliances is authenticated using shared message counters maintained by both the sender and the receiver, the counters is non-

resettable. It is well known in the network security art that circumstances such as system failures and lost of network connection disrupt normal sequencing of shared counters/sequence numbers and thus, subsequent valid messages are still be rejected. Since the claimed shared counters are non-resettable and the disclosure fails to teach any procedure to reset or resynchronize the shared counters/sequence numbers in such situations, the disclosure fails to enable one skilled in the art to make and use the claimed invention. Claim 30 is rejected on the same basis as claim 25. Claims that are not specifically addressed are rejected by virtue of their dependencies.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 16-19, 24 and 28-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sharrow (6,061,668) in view of Elgamal et al (5,825,890) and Hoffman et al (6,366,682).

Sharrow discloses an appliance communication network in which an appliance communication center communicates with different appliances (Abstract; fig. 1, elements 10 and 12-15).

Regarding claim 16, Sharrow discloses a method comprising: applying at an appliance communication center an appliance message to an algorithm to generate a checksum value (fig. 2), and transmitting the appliance message and the checksum value to an appliance (fig. 2). Sharrow does not disclose using a shared message counter shared between the communication center and the appliance, generating an authentication word using the message and the value of the shared message counter and using a separated shared message counter shared between the communication center and another appliance. Elgamal discloses a method for authenticating a message using a message authentication code (MAC). The Elgamal method includes, among other steps, maintaining a shared sequence number, which meets the limitation of a shared message counter, at both ends of a communication channel (col. 18, lines 24-30), applying both a message and a shared message counter to an authentication algorithm to generate an authentication word (col. 17, line 56 – col. 18, line 6), and transmit the first authentication word with the message to a receiver (col. 18, lines 31-38). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the Elgamal method for authenticating a message using a message authentication code into the method of Sharrow; in particular, it would have been obvious to one of ordinary skill in the art at the time the invention was made to maintain a shared message counter at the appliance communication center and the appliance, to apply both the message and a shared message counter to an authentication algorithm to generate an authentication word, and to transmit the

authentication word with the message. The motivation for doing so would have been to allow the receiver of a message to authenticate the message.

Elgamal discloses maintaining a shared message counter in one-to-one communication. Elgamal does not disclose maintaining multiple shared message counters by an entity when the entity communicates with two or more other entities; each of the shared message counters is separately maintained for each of the other entities. Hoffman discloses that an entity (i.e., the data processing center) communicates with other entities (BIA devices) and that the entity maintains multiple shared message counters, each of the shared message counter is separately maintained for each of the other entities (fig. 8; col. 29, line 42 – col. 30, line 59). Since the Sharrow appliance communication center communicates with multiple appliances, it would have been obvious to one of ordinary skill in the art at the time the invention was made to further modify the Sharrow method to maintain, at the appliance communication center, multiple shared message counters, each of the shared message counter is separately maintained for each of the devices, as taught by Hoffman. The motivation for doing so would have been to prevent replay attack when one entity communicates with two or more other entities.

Regarding claim 17, Sharrow further discloses receiving the message at the first appliance (fig. 2; col. 3, lines 23-26). Elgamal further discloses applying the shared message counter, as stored in the receiving side, and the received message to an authentication algorithm to generate a second authentication word and comparing the

first and second authentication words to determine the authenticity of the message (col. 18, lines 31-38).

Regarding claim 18, Elgamal further discloses incrementing the shared message counter, as stored in the receiving side, after receiving a genuine authenticated message at the receiving side (col. 18, lines 24-33).

Regarding claim 19, Elgamal further discloses using a random number in combination with a sequence number, the random number meets the limitation of an authentication keying variable (col. 18, lines 20-23).

Regarding claim 24, Elgamal further discloses incrementing the shared message counter, as stored in the sending side, after transmitting the authenticated message (col. 18, lines 24-30).

Claim 28 is rejected on the same basis as claim 17.

Claim 29 is rejected on the same basis as claim 18.

7. Claims 25, 27 and 30-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sharrow in view of Elgamal, Hoffman and "Commercial Laundry Services".

Regarding claim 25, Sharrow discloses a system in which an appliance communication center is connected to and communicates with a plurality of appliances via a network (fig. 1). Sharrow does not disclose that the appliance communication center uses and stores a shared message counter shared between the communication center and one of the appliances, generating an authentication word using the message

and the value of the shared message counter, using a separated shared message counter shared between the communication center and each of the appliances, and the counters configured to be non-resettable. Elgamal discloses a method for authenticating a message using a message authentication code (MAC). The Elgamal method includes, among other steps, storing a shared sequence number, which meets the limitation of a shared message counter, at both ends of a communication channel (col. 18, lines 24-30), applying both a message and a shared message counter to an authentication algorithm to generate an authentication word (col. 17, line 56 – col. 18, line 6), and transmit the first authentication word with the message to a receiver (col. 18, lines 31-38). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the Elgamal method for authenticating a message using a message authentication code into the system of Sharrow; in particular, it would have been obvious to one of ordinary skill in the art at the time the invention was made to store a shared message counter at the appliance communication center and the appliance, to apply both the message and a shared message counter to an authentication algorithm to generate an authentication word, and to transmit the authentication word with the message. The motivation for doing so would have been to allow the receiver of a message to authenticate the message.

Elgamal discloses maintaining a shared message counter in one-to-one communication. Elgamal does not disclose maintaining multiple shared message counters by an entity when the entity communicates with two or more other entities; each of the shared message counters is separately maintained for each of the other

entities. Hoffman discloses that an entity (i.e., the data processing center) communicates with other entities (BIA devices) and that the entity maintains multiple shared message counters, each of the shared message counter is separately maintained for each of the other entities (fig. 8; col. 29, line 42 – col. 30, line 59). Since the Sharrow appliance communication center communicates with multiple appliances, it would have been obvious to one of ordinary skill in the art at the time the invention was made to further modify the Sharrow method to maintain, at the appliance communication center, multiple shared message counters, each of the shared message counter is separately maintained for each of the devices, as taught by Hoffman. The motivation for doing so would have been to prevent replay attack when one entity communicates with two or more other entities.

Elgamal and Hoffman do not disclose that their counters are non-resettable. The "Commercial Laundry Services" reference discloses using non-resettable counter to insure accountability (see At Jetz, Security is a key). It would have been obvious to one of ordinary skill in the art at the time the invention was made to further modify the Sharrow system such that the counters are non-resettable, as taught in "Commercial Laundry Services", in order to insure accountability.

Regarding claim 27, Elgamal further discloses incrementing the shared message counter, as stored in the sending side, after transmitting the authenticated message (col. 18, lines 24-30).

Regarding claim 30, Sharrow discloses a method comprising: at an appliance, applying an appliance message to an algorithm to generate a checksum value (fig. 3),

and transmitting the appliance message and the checksum by the appliance to an appliance communication center (fig. 3). Sharrow does not disclose maintaining a non-resettable shared message counter at the first appliance and the appliance communication center, using the shared message counter to generate the authentication word, and maintaining multiple non-resettable shared message counters at the appliance communication center, each of the shared message counter is separately maintained for each of the appliances. Elgamal discloses a method for authenticating a message using a message authentication code (MAC). The Elgamal method includes, among other steps, maintaining a shared sequence number, which meets the limitation of a shared message counter, at both ends of a communication channel (col. 18, lines 24-30), applying both a message and a shared message counter to an authentication algorithm to generate an authentication word (col. 17, line 56 – col. 18, line 6), and transmit the authentication word with the message to a receiver (col. 18, lines 31-38). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the Elgamal method for authenticating a message using a message authentication code into the method of Sharrow; in particular, it would have been obvious to one of ordinary skill in the ad at the time the invention was made to maintain a shared message counter at the first appliance and the appliance communication center, to apply both the message and a shared message counter to an authentication algorithm to generate an authentication word, and to transmit the authentication word with the message. The motivation for doing so would have been to allow the receiver of a message to authenticate the message.

Elgamal further discloses using a separate shared counter for transmission direction (i.e., each pair of communication entities) (col. 18; lines 24-27). Since the Sharrow appliance communication center has different transmission directions (i.e., communicates with different appliances) (fig. 1, elements 10 and 12-15), it would have been obvious to one of ordinary skill in the art at the time the invention was made to maintain, at the appliance communication center, a separate shared message counter for each of the appliances because shared messages counters are specific to a particular pair of communication entities, as taught by Elgamal.

Elgamal and Hoffman do not disclose that their counters are non-resettable. The "Commercial Laundry Services" reference discloses using non-resettable counter to insure accountability (see At Jetz, Security is a key). It would have been obvious to one of ordinary skill in the art at the time the invention was made to further modify the Sharrow system such that the counters are non-resettable, as taught in "Commercial Laundry Services", in order to insure accountability.

Regarding claim 31, Sharrow further discloses receiving the message at the appliance communication center (fig. 2; col. 3, lines 23-26). Elgamal further discloses applying the shared message counter, as stored in the receiving side, and the received message to an authentication algorithm to generate a second authentication word and comparing the first and second authentication words to determine the authenticity of the message (col. 18, lines 31-38).

8. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sharrow in view of Elgamal and Hoffman as applied to claim 19 above, and further in view of Kaufman et al ("Network Security Private Communication in a Public World"). Sharrow and Elgamal disclose using a shared message counter to generate the first authentication word in claim 16. Elgamal discloses that the authentication algorithm iteratively performs arithmetic or logical operations (col. 18, lines 4-6). Sharrow and Elgamal do not disclose using a directional code to generate the first authentication word, Kaufman teaches using a directional code for authentication (Section 9.3.5 Privacy and Integrity, p. 242, 3rd par). It would have been obvious to one of ordinary skill in the ad at the time the invention was made to modify the combined method of Sharrow, Elgamal and Hoffman to use a directional code for authentication, as taught by Kaufman. Accordingly, the directional code is used to generate the first authentication word. The motivation for doing so would have been to be able to prevent a reflection attack. Sharrow discloses a working register (col. 5, lines 1-5). Sharrow does not disclose that the working register comprising at least four bytes, the first three bytes holding the shared message counter the fourth byte holding the directional code. However, the differences between the claimed working register and the working register of Sharrow is a matter of design choice since both store the shared message counter and the directional code.

Allowable Subject Matter

9. Claims 21-22 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

10. The following is a statement of reasons for the indication of allowable subject matter. Regarding claim 21, the limitations "forming P as the dot product of R2 and R0; forming Q as the bitwise exclusive or of P with the constant expression '01010101'; forming S by adding Q to K; forming S' by end around rotating S; forming T as the bitwise exclusive or of S' and R3; forming F as the bitwise exclusive or of T with a byte of the appliance message; and replacing R3 with R2, R2 with R1, R1 with R0, and R0 with F", in combination with elements of the parent claims, have not been taught by prior art.

Conclusion

11. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MD

Minh Dinh
Examiner
Art Unit 2132

MD
8/18/05

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100